REMARKS/ARGUMENTS

The Office Action has been carefully considered. Claims 7, 20-30, 37, 40, 53, and 55 are canceled. Claims 1-6, 8-19, 31-36, 38-39, 41-52, 54, and 56-61 are pending.

The Office Action rejected Claims 1-61 in the following manner.

1. Claims 1-4, 8-9, 11-24, 26-31, 34-39, 41-42, 44-52, 54, 56-57, 59, and 61 were rejected under 35 U.S.C. § 103(a) as being obvious considering Published U.S. Patent App. No. 2003/0046238 to Nonaka et al. ("*Nonaka*") in view of U.S. Patent No. 7,062,500 to Hall et al. ("*Hall*") and further in view of Published U.S. Patent App. No. 2002/0152393 to Thoma et al. ("*Thoma*").
2. Claims 5-7, 25, 40, 53, and 55 were rejected under 35 U.S.C. § 103(a) as being obvious considering *Nonaka*, *Hall*, *Thoma* and further in view of U.S. Patent No. 6,959,384 to Serret-Avila et al. ("*Serret-Avila*").
3. Claims 10, 32-33, 43, and 58 were rejected under 35 U.S.C. § 103(a) as being obvious considering *Nonaka*, *Hall*, *Thoma* and further in view of U.S. Patent No. 7,080,043 to Chase, Jr. et al. ("*Chase*").

Claims 1-6, 9, 11-14, 17-18, 31, 34-36, 38-39, 41-42, 45, 47, 49-52, 54, 57, and 60-61 are currently amended, independent Claims 1, 20, 31, 34, and 49 significantly so. For reasons discussed below, Applicants believe that the rejections in the Office Action are moot in light of the current amendments.

35 U.S.C. § 103 Rejections

Nonaka in view of Hall and Thoma does not teach or suggest the elements of Claims 1-4, 8-9, 11-24, 26-31, 34-39, 41-42, 44-52, 54, 56-57, 59, and 61.

Claims 1-4, 8-9, 11-24, 26-31, 34-39, 41-42, 44-52, 54, 56-57, 59, and 61 were rejected under 35 U.S.C. § 103(a) as being obvious considering *Nonaka* in view of *Hall* and further in view of *Thoma*. Applicants respectfully submit that these references, alone or in combination, do not teach or suggest each and every element of Claims 1-4, 8-9, 11-24, 26-31, 34-39, 41-42, 44-52, 54, 56-57, 59, and 61 as currently amended. Amended Claim 1 recites as follows (emphasis added):

> A method comprising:
>
> obtaining clear form rights information at a client device, said clear form rights information being associated with content stored at said client device;

obtaining a **clear form external integrity hash of first data comprising said clear form rights information and an external key as an integrity secret**;

obtaining an **internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key**;

encrypting said internal integrity hash using said externally inaccessible client device key; and

storing the encrypted internal integrity hash on the client device.

The current amendments are intended in part to clarify the internal distinctions between the external integrity hash and the internal integrity hash. These distinctions may be summarized as follows:

1. external integrity hash—remains in clear form; is a hash of data comprising:
   A. rights information and
   B. an external key
2. internal integrity hash—is ultimately encrypted; is a hash of data comprising:
   A. rights information,
   B. the external integrity hash, and
   C. a client device key.

These elements may have been unclearly stated in previous claims. Applicants believe that the combination of these elements, along with the remainder of the claim, is patentably distinct over the prior art. While the prior art abounds with references to well known general concepts such as integrity hashes, clear form data, and secrets of various types, neither *Nonaka*, *Hall*, nor *Thoma*, alone or in combination, teaches or suggests the specific combination of elements that are claimed in Claim 1.

The Office Action correctly asserts that *Nonaka* does not teach or suggest clear form rights information. Applicants respectfully submit that *Nonaka* further does not teach or suggest "obtaining a clear form external integrity hash of first data comprising said clear form rights information and an external key as an integrity secret," as claimed in Claim 1. *Hall* does not remedy this defect. *Hall* discloses merely "machine readable descriptive data structures [that] may be encrypted in whole or in part, while others might be maintained in 'clear' form so that they are easily accessible." *Hall* col. 6 lines 19-22. However, *Hall* goes on to disclose that such data structures do not themselves constitute "rights information," as claimed in Claim 1, but may merely be packaged alongside such rights information: "The machine readable descriptive data structures may themselves be packaged within rights management data structures, and rules (e.g., permissions records) controlling their access and use may be associated with them." *Hall* col. 6 lines 28-32. Thus, *Hall* does not teach or suggest

"clear form rights information at a client device," let alone obtaining a clear form external integrity hash of first data comprising said clear form rights information and an external key as an integrity secret," as claimed in Claim 1. *Thoma* does not remedy this defect.

Furthermore, neither *Nonaka*, *Hall*, nor *Thoma*, alone or in combination, teaches or suggests "obtaining an internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key," as claimed in Claim 1. As discussed above, the cited references do not teach or suggest a "clear form external integrity hash," let alone an "internal integrity hash" of data comprising that external hash along with the rights information and an externally inaccessible client device key.

Although no longer completely on point, Applicants also wish to address the Office Action's assertion at 8 that *Nonaka* teaches determining an integrity hash from rights information and a client device key. In support of that assertion, the Office Action cites to *Nonaka* ¶ [27], which discloses in pertinent part that there is a "hash-value generating circuit… for generating hash values of the content data, the content key data and the UCP data" (emphasis added). Applicants cannot discern how this passage (or any other) in *Nonaka* could plausibly be read to teach or suggest a client device key, let alone an externally inaccessible client device key, as claimed in Claim 1. The Office Action asserts that ¶ [27] of *Nonaka* discloses a "license (i.e. device) key." However, the plain language of ¶ [27] clearly does not even mention a "license key." Moreover, even if *Nonaka* did teach or suggest a "license key," a license key cannot be said to be analogous to an externally inaccessible client device key, as claimed in Claim 1.

Applicants also wish to address the Office Action's assertion at 13 that *Nonaka* discloses an integrity hash generated using an external key as an integrity secret. This assertion remains pertinent to amended Claim 1's recitation of a "clear form external integrity hash of first data comprising said clear form rights information and an external key as an integrity secret." In support of its assertion, the Office Action cites to ¶ [22] of *Nonaka*, which recites in pertinent part, that a "data processing apparatus… encrypts the decrypted content key data and content data by using the session key data," the session key data being external. However, this passage makes clear that *Nonaka* discloses merely that external session key data is used to encrypt content data. By contrast, Claim 1 claims that an external key is combined with rights information (not content data) and is hashed (not encrypted).

It is well known in the art that hashing is a distinct process from encrypting. For example, an "integrity hash" as used in Claim 1 refers to "[a] small amount of binary data… derived… by using a hashing algorithm. The hashing procedure is one-way. There is no feasible way of deriving the

original message... from the hash value...." *See* Harry Newton, *Newton's Telecom Dictionary*, 322-23 (17th ed. 2001) (emphasis added). By contrast, "encryption" as disclosed in *Nonaka* refers to a two-way process: "The transformation of data into a form unreadable by anyone without a secret decryption key." *Id.* at 250. Thus *Nonaka*, alone or in combination with *Hall* and/or *Thoma*, fails to teach or suggest "obtaining a clear form external integrity hash of first data comprising said clear form rights information and an external key as an integrity secret," as claimed in Claim 1.

The Office Action also incorrectly asserts at 13 that *Nonaka* discloses a second integrity hash. This incorrect assertion is relevant to amended Claim 1, which claims both an external and an internal integrity hash. In support of its assertion that *Nonaka* discloses a second integrity hash, the Office Action cites to the exact same passage that was previously said to disclose a first integrity hash, namely, ¶ [27] which discloses which discloses in pertinent part merely that there is a "hash-value generating circuit... for generating hash values...." With respect, Applicants submit that *Nonaka* discloses at most only a circuit that is theoretically capable of generating a second integrity hash. *Nonaka* does not actually ever teach or suggest that it is useful or desirable to generate a second integrity hash. Needless to say, *Nonaka*, alone or in combination with *Hall* and/or *Thoma*, certainly does not teach or suggest "obtaining an internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key," as claimed in Claim 1.

For at least the reasons just discussed, Applicants respectfully submit that Claim 1 as presently amended is not obvious considering *Nonaka* in view of *Hall* and further in view of *Thoma*. Applicants also respectfully submit that Claims 2-4, 8-9, 11-24, 26-31, 34-39, 41-42, 44-52, 54, 56-57, 59, and 61, which include elements similar to those discussed above, are allowable at least by similar reasoning and/or by dependency.

Nonaka in view of Hall, Thoma, and Serret-Avila do not teach or suggest every element of Claims 5-7, 25, 40, 53, and 55.

Claims 5-7, 25, 40, 53, and 55 were rejected under 35 U.S.C. § 103(a) as being obvious considering *Nonaka* in view of *Hall*, *Thoma,* and further in view of *Serret-Avila*. Applicants respectfully submit that these references, alone or in combination, do not teach or suggest each and every element of Claims 5-7, 25, 40, 53, and 55 as currently amended.

The *Serret-Avila* rejections are believed pertinent to the following element of amended Claims 1, 34, and 49: "obtaining an internal integrity hash of second data comprising said clear form

rights information, said clear form external integrity hash, and an externally inaccessible client device key." Claims 5-7, 25, 40, 53, and 55 include by dependency the same or a similar element.

The Office Action is correct insofar as it asserts that *Nonaka* in view of *Hall* does not teach or suggest the capability to generate a second integrity hash using a first integrity hash. The Office Action is also correct insofar as it asserts that *Serret-Avila* discloses the general concept of using a first integrity hash as part of a second integrity hash. *See, e.g.,* col. 4 lines 4-7 ("[A] multi-level hierarchy of hash values is generated… where the hash values on a first level of the hierarchy are at least partially derived from the hash values on a second level of the hierarchy."). However, *Serret-Avila* fails to disclose the specific element claimed in Claim 1 and other independent claims, namely, "obtaining an internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key."

The Office Action asserts at 29 and 30 that *Serret-Avila* discloses generating a hash from rights information and a client device key. However, this assertion appears to be completely unfounded. Indeed, *Serret-Avila* does not even mention hashing a client device key, let alone an externally inaccessible client device key. Nor does *Serret-Avila* even mention hashing rights information, let alone clear form rights information. On the contrary, *Serret-Avila* is entirely directed towards hashing content blocks of a content file. *See, e.g.,* Fig. 4, col. 4 lines 41-48 ("[A] method is disclosed for encoding a digital file… to facilitate secure quasi-random access to the file. [A] multi-level hierarchy of hash values is generated from the digital file, where the hash values on a first level of the hierarchy are at least partially derived from the hash values on a second level of the hierarchy.").

As a basis for its unfounded assertion, the Office Action appears to rely entirely on *Serret-Avila's* general disclosure that a hash may be generated from another hash. However, disclosure of that generic concept cannot be said to teach or suggest generating a hash from rights information and a client device key, let alone "obtaining an internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key," as claimed in the amended claims.

Accordingly, Applicants respectfully submit that *Serret-Avila* does not remedy the acknowledged defects in *Nonaka*, *Hall*, and *Thoma*.

Claims 10, 32-33, 43, and 58

Claims 10, 32-33, 43, and 58 were rejected under 35 U.S.C. § 103(a) as being obvious considering *Nonaka* in view of *Hall*, *Thoma,* and further in view of *Chase*. However, *Chase* is not asserted to and does not in fact remedy any of the above-discussed defects in *Nonaka*, *Hall*, *Thoma*, and *Serret-Avila.*

One of ordinary skill would have had no motivation to combine Nonaka, Hall, Thoma, Serret-Avila, and Chase.

Under the Supreme Court's most recent ruling on the matter, it remains important to avoid the use of hindsight reasoning when combining references. *See KSR International Co. v. Teleflex Inc.*, 550 U.S. –, 127 S.Ct. 1727, 1742; *see also Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 36, 86 S.Ct. 684 (warning against a "temptation to read into the prior art the teachings of the invention in issue" and instructing courts to "guard against slipping into the use of hindsight"). That temptation is especially great where, as here, the invention consists of a specific combination of specific embodiments of several generally known concepts.

Applicants respectfully submit that the only way to assert that the pending claims are obvious would be to "engage in a hindsight reconstruction of the claimed invention, using the applicant's structure as a template and selecting elements from references to fill the gaps." *See In re Gorman*, 993 F.2d 982, 18 U.S.P.Q.2d 1885 (1991). Indeed, it is at least conceivable that the prior art may disclose broad teachings generally similar to some of the specific individual elements of the pending claims.

Applicants respectfully submit that only the blueprint provided by Applicants' claims can provide any plausible motivation to pick and choose from among the countless isolated elements from *Nonaka*, *Hall*, *Thoma*, *Serret-Avila*, and *Chase* in the manner asserted in the Office Action. However, it remains strictly forbidden to "use hindsight reconstruction to pick and choose among isolated disclosures in the prior art" to determine that the pending claims are obvious. *See Ecolochem, Inc. v. Southern California Edison Co.*, 227 F.3d 1361, 56 U.S.P.Q.2d 1065 (2000).

For example, consider Claim 1. It strains credulity that it would have been obvious to one of ordinary skill in the art, having no familiarity with Applicants' disclosures, to pick out and combine isolated elements from four unrelated references, namely *Nonaka's* rights information on a content device, *Hall's* clear form descriptive data structures, *Thoma's* device key, and *Serret-Avila's*

hierarchy of hash values. Applicants respectfully submit that only with the benefit of hindsight can one look back in time and piece together these disparate references.

The motivations to combine asserted in the Office Action are at best merely generally self-laudatory statements about each reference. For example, the Office Action asserts that one would have been motivated to combine *Nonaka* with *Hall* because *Hall* asserts that its teachings are able "to ensure data structure integrity, flexibility, interoperability in the management of rights information." The Office Action also asserts that one would have been motivated to combine *Nonaka* with *Thoma* because *Thoma* enables "the selection of the terminal device to receive distribute[d] digital content from a wide variety of devices." Further, *Serret-Avila's* assertion that it allows "fast, secure, and efficient authentication of data streams" is said to have motivated one of ordinary skill to combine that reference with *Nonaka*. Granted, all other things being equal, efficiency, flexibility, and interoperability are generally preferred over inefficiency, inflexibility, and lack of interoperability. However, Claim 1's utility (and novelty) lies in other areas. Claim 1 is not particularly directed towards efficient authentication of data streams (as in *Serret-Avila*) or wide interoperability (as in *Thoma*) or flexibility (as in *Hall*). Indeed, at best the asserted general motivations are only tangentially related to potential side effects of the specific embodiment claimed in Claim 1. At worst, some of the asserted general motivations are simply irrelevant (e.g., *Serret-Avila:* Claim 1 is directed towards using a specific combination of integrity hashes to authenticate rights information, not data streams).

Applicants respectfully submit that nothing in the references or in the art suggests that one of ordinary skill at the time of the invention would have found it obvious to pick and choose all of these isolated individual elements from four merely tangentially related references in order to achieve the specific invention claimed in Claim 1. The remaining claims are also allowable by similar reasoning. Accordingly, Applicants respectfully submit that for this additional reason Claims 1-6, 8-19, 31-36, 38-39, 41-52, 54, and 56-61 are in condition for allowance.

CONCLUSION

For at least the reasons above, Applicants respectfully submit that Claims 1-6, 8-19, 31-36, 38-39, 41-52, 54, and 56-61 are allowable and request that the Examiner permit these claims to proceed to issuance. Although additional arguments are believed to exist for distinguishing the cited documents, the arguments presented are believed sufficient to address the Examiner's rejections. Likewise, failure of the Applicants to respond to a position taken by the Examiner is not an indication of acceptance or acquiescence of the Examiner's position. Instead, it is believed that the Examiner's positions are rendered moot by the foregoing arguments, and it is therefore not believed necessary to respond to every position taken by the Examiner with which Applicants do not agree.

The Examiner is respectfully requested to contact the undersigned at the telephone number below if there are any remaining questions regarding this application.

We believe the appropriate fees accompany this transmission. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to Axios Law Group's deposit account. The deposit account number is 50-4051.

Respectfully submitted,
AXIOS LAW GROUP

Date: April 22, 2008

by: /Adam L.K. Philipp/
Adam L.K. Philipp
Reg. No.: 42,071
Direct: 206.217.2226
E-mail: adam@axioslaw.com

AXIOS Law Group
1525 4th Avenue, Suite 800
Seattle, WA 98101
Telephone: 206-217-2200
Customer No.: 61,857